PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-088431
(43)Date of publication of application : 30.03.1999

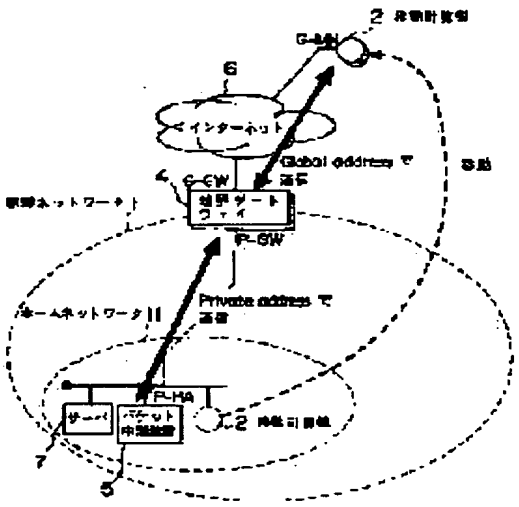
(51)Int.CI. H04L 12/56
G06F 13/00
H04B 7/26
H04L 9/14
// G09C 1/00

(21)Application number : 09-241156
(22)Date of filing : 05.09.1997

(71)Applicant : TOSHIBA CORP
(72)Inventor : INOUE ATSUSHI
ISHIYAMA MASAHIRO
FUKUMOTO ATSUSHI
TSUDA YOSHIYUKI

(54) PACKET RELAY DEVICE, MOVING COMPUTER DEVICE, MOVING COMPUTER MANAGEMENT DEVICE, PACKET RELAY METHOD, PACKET TRANSMISSION METHOD AND MOVING COMPUTER POSITION REGISTRATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To continuously use a moving IP system even if a moving computer moves to a global address out of an organization by inspecting the content of a packet and transferring it as a system using a private address.
SOLUTION: A packet relay device (moving computer management device) 5 receiving a ciphered registration request packet decodes the packet by a key for the moving computer 2 being a transmission source and inspects the contents of the packet. When it is judged to be the registration request of moving IP from identification information in a packet header, the home address and the present position address of the moving computer are taken out from the packet and they are registered in a management table. The payload of a response packet (registration succeeding packet) for the registration request is ciphered with the key corresponding to the moving computer 2 being a transmission destination. The moving computer 2 decodes the packet with the key corresponding to the packet relay device 5 being the transmission source and registration success is recognized from the obtained response packet.



LEGAL STATUS

[Date of request for examination] 19.03.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or

application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－88431

(43)公開日　平成11年(1999)３月30日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｈ０４Ｌ　12/56		Ｈ０４Ｌ　11/20		１０２Ａ
Ｇ０６Ｆ　13/00	３５３	Ｇ０６Ｆ　13/00		３５３Ｃ
Ｈ０４Ｂ　7/26		Ｇ０９Ｃ　1/00		６６０Ｅ
Ｈ０４Ｌ　9/14		Ｈ０４Ｂ　7/26		Ｍ
// Ｇ０９Ｃ　1/00	６６０	Ｈ０４Ｌ　9/00		６４１

審査請求　未請求　請求項の数11　ＯＬ　（全 19 頁）

(21)出願番号　特願平9－241156

(22)出願日　平成９年(1997)９月５日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　井上　淳
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　石山　政浩
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　福本　淳
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(74)代理人　弁理士　鈴江　武彦　（外６名）

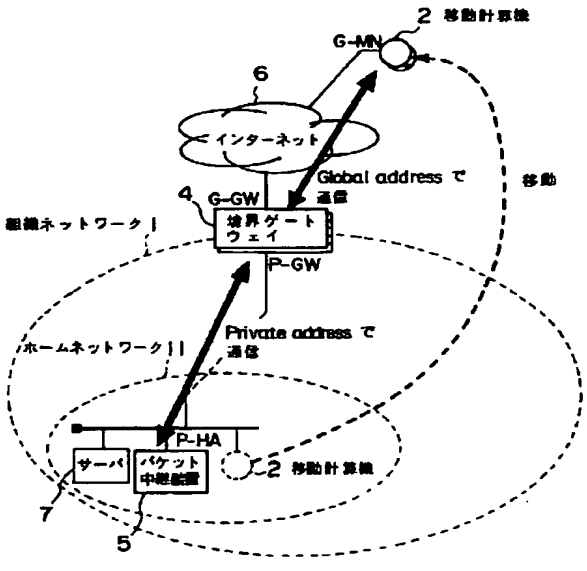
最終頁に続く

(54)【発明の名称】　パケット中継装置、移動計算機装置、移動計算機管理装置、パケット中継方法、パケット送信方法及び移動計算機位置登録方法

(57)【要約】

【課題】　移動計算機が組織外のグローバルアドレスに移動しても移動ＩＰ方式をそのまま使用し続けること可能とするパケット中継装置を提供すること。

【解決手段】　ホームエージェントの属するネットワーク内に設置され、ネットワーク内との通信では内部アドレスを外部との通信では外部アドレスを用い、ネットワーク外に移動した計算機から自身の外部アドレス宛の暗号化パケットを受信し復号して得た内部パケットの宛先計算機宛に、内部パケットを再度暗号化し送信元を自装置の内部アドレス、宛先を宛先計算機のアドレスとするヘッダを付加したパケットを転送し、ネットワーク内の計算機から自身の内部アドレス宛の暗号化パケットを受信し復号して得た内部パケットの宛先移動計算機宛に、内部パケットを再度暗号化し送信元を自装置の外部アドレス、宛先を移動計算機の現在位置アドレスとするヘッダを付加したパケットを転送する。



1

【特許請求の範囲】

【請求項１】ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し、該移動計算機宛のパケットを該移動計算機の現在位置アドレス宛に転送する手段を有する移動計算機管理装置の設置されたネットワーク内に設置された、ネットワーク内に位置する計算機とネットワーク外に位置する計算機との間で送受信されるパケットを中継するパケット中継装置であって、

前記ネットワーク内部の計算機との間での通信に用いる内部アドレスと、前記ネットワーク外部の計算機との間での通信に用いる外部アドレスとを記憶する第１の記憶手段と、

前記ネットワーク内部に属する各移動計算機の所属アドレス情報、各移動計算機が前記ネットワーク外部に移動した場合の現在位置アドレス情報、および前記ネットワーク外部に移動した各移動計算機との間でのパケット暗号化のための鍵情報を少なくとも対応付けて記憶する第２の記憶手段と、

前記ネットワーク外部に移動した移動計算機から送信された暗号化パケットを対応する前記鍵情報を用いて復号し、得られた内部パケットの宛先となる計算機宛に、該内部パケットを再度暗号化し、さらに送信元を自装置の内部アドレス、宛先を該宛先計算機のアドレスとするヘッダを付加して得たパケットを転送する手段と、

前記ネットワーク内部の計算機から送信された暗号化パケットを復号し、得られた内部パケットの宛先となる移動計算機に対応する前記鍵情報で該内部パケットを再度暗号化し、さらに送信元を自装置の外部アドレス、宛先を該移動計算機の現在位置アドレスとするヘッダを付加して、該移動計算機に転送する手段とを備えたことを特徴とするパケット中継装置。

【請求項２】前記ネットワーク外部に移動した移動計算機から送信された暗号化パケットを復号して得た前記内部パケットが、前記移動計算機管理装置宛の現在移動アドレス情報を含む登録要求パケットである場合、該現在移動アドレス情報を前記第２の記憶手段に登録する手段をさらに備えたことを特徴とする請求項１に記載のパケット中継装置。

【請求項３】相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、

自装置の移動位置情報を管理し自装置宛のパケットを自装置の現在位置アドレス宛に転送する移動計算機管理装置宛に直接パケットを送信することが可能な、該移動計算機管理装置の設置されたネットワークと同じアドレス空間に自装置が接続しているか否かを示す情報を記憶する手段と、

自装置を対象とする前記移動計算機管理装置の設置されたネットワークと異なるアドレス空間と、該ネットワークと同じアドレス空間との境界に設置され、アドレス空間ごとに設定されたアドレスを用いて、両アドレス空間にそれぞれ接続された計算機間で送受信されるパケットを中継するパケット中継装置の、該異なるアドレス空間におけるアドレスを記憶する手段と、

自装置が前記移動計算機管理装置の設置されたネットワークと異なるアドレス空間に接続していることを示す情報が記憶されている場合、該移動計算機管理装置宛の現在移動アドレス情報を含む登録要求パケットを、前記パケット中継装置宛に暗号化して送信する手段とを備えたことを特徴とする移動計算機装置。

【請求項４】相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、

自装置の移動位置情報を管理し自装置宛のパケットを自装置の現在位置アドレス宛に転送する移動計算機管理装置宛に直接パケットを送信することが可能な、該移動計算機管理装置の設置されたネットワークと同じアドレス空間に、自装置が接続しているか否かを示す情報を記憶する手段と、

自装置を対象とする前記移動計算機管理装置の設置されたネットワークと異なるアドレス空間と、該ネットワークと同じアドレス空間との境界に設置され、アドレス空間ごとに設定されたアドレスを用いて、両アドレス空間にそれぞれ接続された計算機間で送受信されるパケットを中継するパケット中継装置の、該異なるアドレス空間におけるアドレスを記憶する手段と、

自装置が前記移動計算機管理装置の設置されたネットワークと異なるアドレス空間に接続していることを示す情報が記憶されている場合、該ネットワーク内に位置する計算機を宛先とするパケット全体を暗号化して前記パケット中継装置宛に送信する手段とを備えたことを特徴とする移動計算機装置。

【請求項５】移動先におけるアドレスを自動取得するか否かを設定する手段と、

自装置が前記移動計算機管理装置の設置されたネットワークと異なるアドレス空間に接続していることを示す前記設定がされている場合に、前記アドレスを自動取得することを示す設定がされているならば、アドレスの割当てを受けるための所定のプロトコルを実行して取得したアドレスを自装置の現在位置アドレスとする手段とをさらに備えたことを特徴とする請求項３または４に記載の移動計算機装置。

【請求項６】ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し、該移動計算機宛のパケットを該移動計算機の現在位置に転送する手段を有するパケット中継装置であって、

自装置の属するネットワーク内部に属する各移動計算機の所属アドレス情報および各移動計算機が該ネットワーク外部に移動した場合の現在位置アドレス情報を少なくとも対応付けて記憶する記憶手段と、

自装置の属するネットワークと同じアドレス空間と、該

アドレス空間とは異なるアドレス空間との境界に設置され、アドレス空間ごとに設定されたアドレスを用いて、両アドレス空間にそれぞれ接続された計算機間で送受信されるパケットを中継するパケット中継装置から中継されてきた暗号化パケットを復号し、得られた内部パケットが自装置の管理対象とする移動計算機から自装置宛に発せられた現在移動アドレス情報を含む登録要求パケットである場合、該現在移動アドレス情報を前記記憶手段に登録する手段とを備えたことを特徴とするパケット中継装置。

【請求項７】前記登録要求パケットに対する前記移動計算機宛の登録応答パケットを、前記パケット中継装置宛に暗号化して送信する手段をさらに備えたことを特徴とする請求項６に記載のパケット中継装置。

【請求項８】自装置の属するネットワーク外部に移動中の移動計算機の前記所属アドレス宛に転送されてきたパケットを捕捉した場合、該パケットを、送信元を自装置のアドレス、宛先を該移動計算機の該所属アドレスとするパケットにカプセル化した後に、さらにこのカプセル化されたパケットを、前記パケット中継装置宛に暗号化して送信する手段をさらに備えたことを特徴とする請求項６または７に記載のパケット中継装置。

【請求項９】ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し、該移動計算機宛のパケットを該移動計算機の現在位置アドレス宛に転送する手段を有する移動計算機管理装置の設置されたネットワーク内に設置された、ネットワーク内に位置する計算機とネットワーク外に位置する計算機との間で送受信されるパケットを中継するとともに、該ネットワーク内部の計算機との間での通信には内部アドレスを用い、該ネットワーク外部の計算機との間での通信には外部アドレスを用いるパケット中継装置におけるパケット中継方法であって、

前記ネットワーク外部に移動した移動計算機から自装置の外部アドレス宛に送信された暗号化パケットを受信した場合、この暗号化パケットを対応する鍵情報を用いて復号し、得られた内部パケットの宛先となる計算機宛に、該内部パケットを再度暗号化し、さらに送信元を自装置の内部アドレス、宛先を該宛先計算機のアドレスとするヘッダを付加して得たパケットを転送するとともに、

前記ネットワーク内部の計算機から自装置の内部アドレス宛に送信された暗号化パケットを受信した場合、該暗号化パケットを復号し、得られた内部パケットの宛先となる移動計算機に対応する鍵情報で該内部パケットを再度暗号化し、さらに送信元を自装置の外部アドレス、宛先を該移動計算機の現在位置アドレスとするヘッダを付加して、該移動計算機に転送する手段とを備えたことを特徴とするパケット中継方法。

【請求項１０】相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置におけるパケット送信方法であって、

自装置の移動位置情報を管理し自装置宛のパケットを自装置の現在位置アドレス宛に転送する移動計算機管理装置の属するネットワーク内に位置する計算機を宛先とするパケットを送信する場合、該移動計算機管理装置の設置されたネットワークと同じアドレス空間に自装置が接続されていないことを示す情報が設定されているならば、

自装置を対象とする前記移動計算機管理装置の設置されたネットワークと異なるアドレス空間と、該ネットワークと同じアドレス空間との境界に設置され、アドレス空間ごとに設定されたアドレスを用いて、両アドレス空間にそれぞれ接続された計算機間で送受信されるパケットを中継するパケット中継装置の、該異なるアドレス空間におけるアドレス宛に、該ネットワークにおける自装置および宛先計算機のアドレスを含むパケット全体を暗号化して送信することを特徴とするパケット送信方法。

【請求項１１】ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し、該移動計算機宛のパケットを該移動計算機の現在位置に転送する手段を有するパケット中継装置における移動計算機登録方法であって、

自装置の属するネットワークと同じアドレス空間と、該アドレス空間とは異なるアドレス空間との境界に設置され、アドレス空間ごとに設定されたアドレスを用いて、両アドレス空間にそれぞれ接続された計算機間で送受信されるパケットを中継するパケット中継装置から中継されてきた暗号化パケットを受信した場合、該暗号化パケットを復号し、

得られた内部パケットが自装置の管理対象とする移動計算機から自装置宛に発せられた現在移動アドレス情報を含む登録要求パケットである場合、該現在移動アドレス情報を登録することを特徴とする移動計算機登録方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、相互接続している複数のネットワーク上を移動しながら通信を行う移動計算機及びその移動計算機を宛先または送信元とするデータパケットを中継するパケット中継装置並びにパケット中継方法、パケット送信方法及び移動計算機登録方法に関する。

【０００２】

【従来の技術】計算機システムの小型化、低価格化やネットワーク環境の充実に伴って、計算機システムの利用は急速にかつ種々の分野に広く拡大し、また集中型システムから分散型システムへの移行が進んでいる。特に近年では計算機システム自体の進歩、能力向上に加え、コンピュータ・ネットワーク技術の発達・普及により、オフィス内のファイルやプリンタなどの資源共有のみなら

ず、オフィス外、一組織外とのコミュニケーション（電子メール、電子ニュース、ファイルの転送など）が可能になり、これらが広く利用されはじめた。特に近年では、世界最大のコンピュータネットワーク「インターネット（ｉｎｔｅｒｎｅｔ）」の利用が普及しており、インターネットと接続し、公開された情報、サービスを利用したり、逆にインターネットを通してアクセスしてくる外部ユーザに対し、情報、サービスを提供することで、新たなコンピュータビジネスが開拓されている。また、インターネット利用に関して、新たな技術開発、展開がなされている。

【０００３】また、このようなネットワークの普及に伴い、移動通信（ｍｏｂｉｌｅ　ｃｏｍｐｕｔｉｎｇ）に対する技術開発も行われている。移動通信では、携帯型の端末、計算機を持ったユーザがネットワーク上を移動して通信する。ときには通信を行いながらネットワーク上の位置を変えていく場合もあり、そのような通信において変化する移動計算機のネットワーク上を管理し、正しく通信内容を到達させるための方式が必要である。

【０００４】一般に移動通信を行う場合、移動計算機が所属していたネットワークに移動計算機の移動先データを管理するルータ（ホームエージェント）を置き、移動計算機が移動した場合、このホームエージェントに対して現在位置を示す登録メッセージを送る。登録メッセージが受け取られたら、移動計算機宛データの送信はそのホームエージェントを経由して、移動計算機の元のアドレス宛のＩＰパケットを移動計算機の現在位置アドレス宛パケット内にカプセル化することで移動計算機に対するデータの経路制御が行われる。例えば、図６では、元々ホームネットワーク１０１ａに属していた移動計算機１０２が、他のネットワーク１０１ｂに移動し、ネットワーク１０１ｃ内の他の計算機（ＣＨ）１０３との間で通信を行う場合に、移動計算機１０２に対しホームエージェント（ＨＡ）１０５が上記の役割を行う。この方式は、インターネットの標準化団体であるＩＥＴＦのｍｏｂｉｌｅ－ＩＰワーキンググループで標準化が進められている移動ＩＰと呼ばれる方式である（文献：ＲＦＣ２００２，　ＩＰ　ｍｏｂｉｌｉｔｙ　ｓｕｐｐｏｒｔ（Ｃ．Ｐｅｒｋｉｎｓ））。

【０００５】また、ネットワークが普及し、ネット間の自由な接続が実現され、膨大なデータ、サービスのやりとりがなされる場合、セキュリティ上の問題を考慮する必要が生じてくる。例えば組織内部の秘密情報の外部ネットワークへの漏洩をいかに防ぐか、という問題や、組織外からの不正な侵入から、組織内ネットワークに接続された資源、情報をいかに守るか、という問題である。インターネットは、当初学術研究を目的に構築されたため、ネットワークの接続による自由なデータサービスのやりとりを重視しており、このようなセキュリティ上の問題は考慮されていなかったが、近年多くの企業、団体

がインターネットに接続するようになり、セキュリティ上の問題から自組織ネットワークを防衛する機構が必要となってきた。

【０００６】そこで、インターネット上でデータパケットを交換する際に、外部にデータパケットを送出する前にその内容を暗号化し認証コードをつけ、受信したサイトで認証コードを確認し復号化する、という方法がある。この方法によれば、たとえ組織外のユーザが外部ネットワーク上のデータパケットを取り出しても、内容が暗号化されているので、決してその内部が漏洩することがなく、安全な通信が確保できる。

【０００７】このような暗号化通信をサポートするゲートウェイ計算機で守られた（ガードされた）ネットワーク同士であれば相互に暗号化通信が可能であり、また前述の移動計算機が自分でパケットの暗号化、復号を行う機能をサポートしていれば、任意のゲートウェイ間、またはゲートウェイ～移動計算機間で暗号化通信がサポートできる。例えば図６では、元々ホームネットワーク１０１ａに属していた移動計算機１０２が、他のネットワーク１０１ｂに移動し、ネットワーク１０１ｃ内の他の計算機（ＣＨ）１０３と暗号化、復号機能をサポートするゲートウェイ１０４ａ，１０４ｃを介して暗号化通信を行う。

【０００８】図６では、移動ＩＰとパケット暗号化を併用して通信を行う場合、パケットの転送経路は、

ＣＨ→ゲートウェイ１０４ｃ→ゲートウェイ１０４ａ→ホームエージェント（ＨＡ）１０５→ゲートウェイ１０４ａ→移動計算機１０２

となり、ゲートウェイ４ａでは、一旦パケットは復号されてホームエージェント１０５に送られ、その後、再度ホームエージェント１０５発のパケットが暗号化される。

【０００９】さて、移動ＩＰ方式では、単一のアドレス空間上を移動計算機が移動する場合のみを想定して、プロトコルが構成されている。すなわち、移動先からの現在位置の登録メッセージは必ずホームネットのホームエージェントに到達可能であると仮定している。しかし、昨今では大規模な組織がインターネットに接続する場合、ＩＰアドレスの枯渇の問題から、組織内の全てのホストにグローバルＩＰアドレスが割り当てられているのは稀で、組織内はプライベートアドレス（文献：ＲＦＣ１５９７）で運用し、外部に通信する場合は、グローバルアドレスへのアドレス変換を行う場合が多い。

【００１０】その場合、グローバルアドレス領域に移動した移動計算機から、プライベートアドレス領域内のホームエージェントに送信された登録要求パケットは、そのままでは到達可能でない。

【００１１】そこで、このような複数のアドレス空間が混在するネットワーク構成では、組織ネットワークの入口で移動計算機から送信された登録要求パケットを一旦

受信し、内容を確認して、組織内の該当するホームエージェント宛に転送する処理が必要である（移動ＩＰ方式では、ホームエージェントはサブネットに１つ設置されるので、組織内に複数のホームエージェントが置かれることがあるため）。また、移動計算機の側でも、自分がプライベートアドレス領域で移動しているのか、グローバルアドレス領域に移動したかに応じて、登録要求パケットの内容を変える制御機構が必要になる。

【００１２】以上説明したように、一般に移動ＩＰ方式を利用して移動計算機をサポートする場合、移動計算機が複数のアドレス空間に渡って移動（プライベート→グローバルのように）する場合、移動計算機の現在位置に応じホームネットのホームエージェント宛に送信する登録要求などのパケット形式を制御するための方式や、プライベートネット／グローバルネットの境界である組織入口で、送信されたパケットを一旦受信し、内容を確認して、組織内の該当するホームエージェント宛に転送するための方式が必要になる。

【００１３】

【発明が解決しようとする課題】従来の移動ＩＰ方式では、移動計算機はホームネットワークとの到達可能性（ｒｅａｃｈａｂｉｌｉｔｙ）を仮定してプロトコルを構成していたため、ホームネットワークと共通のアドレス空間内のみを移動するという制約があった。このため、組織がプライベートアドレスで運用された場合、移動計算機が組織ネットワークの外（グローバルアドレス領域）に移動すると、移動ＩＰ方式がそのまま使用できないという欠点があった。

【００１４】本発明は、上記事情を考慮してなされたもので、複数の計算機が複数の相互接続された通信ネットワークにより互いに接続されて相互に通信可能に構成された計算機システムで、移動ＩＰによる移動計算機への自動経路制御がサポートされている場合において、ホームネットワークと異なるアドレス管理領域に移動した移動計算機発の位置登録メッセージなどのパケットを、組織ネットワークの入口で一旦受信し、内容を確認して、組織内の該当するホームエージェント宛に転送する処理を行うと共に、移動計算機側でも自身の現在位置に応じて適切な形式でパケットを生成、送信するような移動計算機制御を可能とするパケット中継装置、移動計算機装置、パケット中継方法、パケット送信方法及び移動計算機登録方法を提供することを目的とする。

【００１５】

【課題を解決するための手段】本発明（請求項１）は、ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し、該移動計算機宛のパケットを該移動計算機の現在位置アドレス宛に転送する手段を有する移動計算機管理装置（ホームエージェント、実施形態におけるパケット中継装置）の設置されたネットワーク内に設置された、ネットワーク内に位置する計

算機（前記移動計算機管理装置も含む）とネットワーク外に位置する計算機（前記移動計算機も含む）との間で送受信されるパケットを中継するパケット中継装置（境界ゲートウェイ）であって、前記ネットワーク内部の計算機との間での通信に用いる内部アドレス（例えばプライベートアドレス）と、前記ネットワーク外部の計算機との間での通信に用いる外部アドレス（例えばグローバルアドレス）とを記憶する第１の記憶手段と、前記ネットワーク内部に属する各移動計算機の所属アドレス情報、各移動計算機が前記ネットワーク外部に移動した場合の現在位置アドレス情報、および前記ネットワーク外部に移動した各移動計算機との間でのパケット暗号化のための鍵情報を少なくとも対応付けて記憶する第２の記憶手段と、前記ネットワーク外部に移動した移動計算機から送信された暗号化パケットを対応する前記鍵情報を用いて復号し、得られた内部パケット（登録要求パケットも含む）の宛先となる計算機宛に、該内部パケットを再度暗号化し、さらに送信元を自装置の内部アドレス、宛先を該宛先計算機のアドレスとするヘッダを付加して得たパケットを転送する手段と、前記ネットワーク内部の計算機（前記移動計算機管理装置も含む）から送信された暗号化パケットを復号し、得られた内部パケット（登録応答パケットも含む）の宛先となる移動計算機に対応する前記鍵情報で該内部パケットを再度暗号化し、さらに送信元を自装置の外部アドレス、宛先を該移動計算機の現在位置アドレスとするヘッダを付加して、該移動計算機に転送する手段とを備えたことを特徴とする。

【００１６】好ましくは、前記ネットワーク外部に移動した移動計算機から送信された暗号化パケットを復号して得た前記内部パケットが、前記移動計算機管理装置宛の現在移動アドレス情報を含む登録要求パケットである場合、該現在移動アドレス情報を前記第２の記憶手段に登録する手段をさらに備えるようにしてもよい。

【００１７】本発明（請求項３）は、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、自装置の移動位置情報を管理し自装置宛のパケットを自装置の現在位置アドレス宛に転送する移動計算機管理装置（ホームエージェント、実施形態におけるパケット中継装置）宛に直接パケットを送信することが可能な、該移動計算機管理装置の設置されたネットワークと同じアドレス（例えばプライベートアドレス）空間に自装置が接続しているか否かを示す情報を記憶する手段と、自装置を対象とする前記移動計算機管理装置の設置されたネットワークと異なるアドレス（例えばグローバルアドレス）空間と、該ネットワークと同じアドレス空間との境界に設置され、アドレス空間ごとに設定されたアドレスを用いて、両アドレス空間にそれぞれ接続された計算機（前記移動計算機、前記移動計算機管理装置も含む）間で送受信されるパケットを中継するパケット中継装置（境界ゲートウェイ）の、該異なる

アドレス空間におけるアドレスを記憶する手段と、自装置が前記移動計算機管理装置の設置されたネットワークと異なるアドレス空間に接続していることを示す情報が記憶されている場合、該移動計算機管理装置宛の現在移動アドレス情報を含む登録要求パケットを、前記パケット中継装置宛に暗号化して送信する手段とを備えたことを特徴とする。

【００１８】本発明（請求項４）は、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、自装置の移動位置情報を管理し自装置宛のパケットを自装置の現在位置アドレス宛に転送する移動計算機管理装置宛に直接パケットを送信することが可能な、該移動計算機管理装置（ホームエージェント、実施形態におけるパケット中継装置）の設置されたネットワークと同じアドレス（例えばプライベートアドレス）空間に、自装置が接続しているか否かを示す情報を記憶する手段と、自装置を対象とする前記移動計算機管理装置の設置されたネットワークと異なるアドレス（例えばグローバルアドレス）空間と、該ネットワークと同じアドレス空間との境界に設置され、アドレス空間ごとに設定されたアドレスを用いて、両アドレス空間にそれぞれ接続された計算機（前記移動計算機、前記移動計算機管理装置も含む）間で送受信されるパケットを中継するパケット中継装置（境界ゲートウェイ）の、該異なるアドレス空間におけるアドレスを記憶する手段と、自装置が前記移動計算機管理装置の設置されたネットワークと異なるアドレス空間に接続していることを示す情報が記憶されている場合、該ネットワーク内に位置する計算機を宛先とするパケット全体を暗号化して前記パケット中継装置宛に送信する手段とを備えたことを特徴とする。

【００１９】好ましくは、移動先におけるアドレスを自動取得するか否かを設定する手段と、自装置が前記移動計算機管理装置の設置されたネットワークと異なるアドレス空間に接続していることを示す前記設定がされている場合に、前記アドレスを自動取得することを示す設定がされているならば、アドレスの割当てを受けるための所定のプロトコル（例えばＰＰＰプロトコル）を実行して取得したアドレスを自装置の現在位置アドレスとする手段とをさらに備えるようにしてもよい。

【００２０】本発明（請求項６）は、ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し、該移動計算機宛のパケットを該移動計算機の現在位置に転送する手段を有するパケット中継装置（実施形態におけるパケット中継装置）であって、自装置の属するネットワーク内部に属する各移動計算機の所属アドレス情報および各移動計算機が該ネットワーク外部に移動した場合の現在位置アドレス情報を少なくとも対応付けて記憶する記憶手段と、自装置の属するネットワークと同じアドレス（例えばプライベートアドレス）空間と、該アドレス空間とは異なるアドレス（例えばグローバルアドレス）空間との境界に設置され、アドレス空間ごとに設定されたアドレスを用いて、両アドレス空間にそれぞれ接続された計算機（前記移動計算機、前記移動計算機管理装置も含む）間で送受信されるパケットを中継するパケット中継装置（境界ゲートウェイ）から中継されてきた暗号化パケットを復号し、得られた内部パケットが自装置の管理対象とする移動計算機から自装置宛に発せられた現在移動アドレス情報を含む登録要求パケットである場合、該現在移動アドレス情報を前記記憶手段に登録する手段とを備えたことを特徴とする。

【００２１】好ましくは、前記登録要求パケットに対する前記移動計算機宛の登録応答パケットを、前記パケット中継装置宛に暗号化して送信する手段をさらに備えるようにしてもよい。

【００２２】好ましくは、自装置の属するネットワーク外部に移動中の移動計算機の前記所属アドレス宛に転送されてきたパケットを捕捉した場合、該パケットを、送信元を自装置のアドレス、宛先を該移動計算機の該所属アドレスとするパケットにカプセル化した後に、さらにこのカプセル化されたパケットを、前記パケット中継装置宛に暗号化して送信する手段をさらに備えるようにしてもよい。

【００２３】本発明（請求項９）は、ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し、該移動計算機宛のパケットを該移動計算機の現在位置アドレス宛に転送する手段を有する移動計算機管理装置の設置されたネットワーク内に設置された、ネットワーク内に位置する計算機とネットワーク外に位置する計算機との間で送受信されるパケットを中継するとともに、該ネットワーク内部の計算機との間での通信には内部アドレスを用い、該ネットワーク外部の計算機との間での通信には外部アドレスを用いるパケット中継装置（境界ゲートウェイ）におけるパケット中継方法であって、前記ネットワーク外部に移動した移動計算機から自装置の外部アドレス宛に送信された暗号化パケットを受信した場合、この暗号化パケットを対応する鍵情報を用いて復号し、得られた内部パケットの宛先となる計算機宛に、該内部パケットを再度暗号化し、さらに送信元を自装置の内部アドレス、宛先を該宛先計算機のアドレスとするヘッダを付加して得たパケットを転送するとともに、前記ネットワーク内部の計算機から自装置の内部アドレス宛に送信された暗号化パケットを受信した場合、該暗号化パケットを復号し、得られた内部パケットの宛先となる移動計算機に対応する鍵情報で該内部パケットを再度暗号化し、さらに送信元を自装置の外部アドレス、宛先を該移動計算機の現在位置アドレスとするヘッダを付加して、該移動計算機に転送する手段とを備えたことを特徴とする。

【００２４】本発明（請求項１０）は、相互に接続され

たネットワーク間を移動して通信を行うことが可能な移動計算機装置におけるパケット送信方法であって、自装置の移動位置情報を管理し自装置宛のパケットを自装置の現在位置アドレス宛に転送する移動計算機管理装置の属するネットワーク内に位置する計算機を宛先とするパケットを送信する場合、該移動計算機管理装置の設置されたネットワークと同じアドレス空間に自装置が接続されていないことを示す情報が設定されているならば、自装置を対象とする前記移動計算機管理装置の設置されたネットワークと異なるアドレス空間と、該ネットワークと同じアドレス空間との境界に設置され、アドレス空間ごとに設定されたアドレスを用いて、両アドレス空間にそれぞれ接続された計算機間で送受信されるパケットを中継するパケット中継装置の、該異なるアドレス空間におけるアドレス宛に、該ネットワークにおける自装置および宛先計算機のアドレスを含むパケット全体を暗号化して送信することを特徴とする。

【００２５】本発明（請求項１１）は、ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し、該移動計算機宛のパケットを該移動計算機の現在位置に転送する手段を有するパケット中継装置（実施形態におけるパケット中継装置）における移動計算機登録方法であって、自装置の属するネットワークと同じアドレス空間と、該アドレス空間とは異なるアドレス空間との境界に設置され、アドレス空間ごとに設定されたアドレスを用いて、両アドレス空間にそれぞれ接続された計算機間で送受信されるパケットを中継するパケット中継装置から中継されてきた暗号化パケットを受信した場合、該暗号化パケットを復号し、得られた内部パケットが自装置の管理対象とする移動計算機から自装置宛に発せられた現在移動アドレス情報を含む登録要求パケットである場合、該現在移動アドレス情報を登録することを特徴とする。

【００２６】なお、以上の各装置に係る発明は方法に係る発明としても成立し、方法に係る発明は装置に係る発明としても成立する。また、上記の発明は、相当する手順あるいは手段をコンピュータに実行させるためのプログラムを記録した機械読取り可能な媒体としても成立する。

【００２７】従来、移動ＩＰ方式では、移動計算機はホームネットワークとの到達可能性（ｒｅａｃｈａｂｉｌｉｔｙ）の保証された単一空間内でのみ移動が許されており、例えば大規模な組織で組織内ネットワークをプライベートアドレスで構築している場合、組織外のグローバルアドレス領域に移動した計算機からは移動ＩＰ方式をそのまま使用できなかった。これに対して本発明によれば、移動計算機側で自身の現在位置に応じて適切な形式でパケットを生成、送信するような制御を可能とし、また、組織ネットワークの入口で移動計算機からのパケットを一旦受信し、内容を確認して、組織内の該当するパケット中継装置（ホームエージェント）宛に転送する処理を行うことにより、例えば企業ネットがプライベートアドレスで運用しており、移動計算機が組織外のグローバルアドレスに移動しても移動ＩＰ方式をそのまま使用し続けることができる。

【００２８】一般に、大規模ネットワークでは、企業ネットの入口で通信内容のログを取ったりすることが多く、パケット中継装置（境界ゲートウェイ）の処理のオーバーヘッドは実際には問題にならない場合が多い。また、パケット中継装置（境界ゲートウェイ）でファイアウォールなどの他の制御機構を共存させる場合も拡張が容易である。

【００２９】また、本発明において、インターネットプロバイダなどに接続するシーケンス内で移動計算機のＩＰネットワーク上の位置を検出することで、移動計算機側の制御をさらに容易にできる。

【００３０】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。図１に、本実施形態に係るネットワークの基本構成を示す。図１では、組織ネットワーク１の中にホームネットワーク１１が存在する。組織ネットワーク（例えば企業内ネットワーク）１全体はプライベートアドレスで運用されている。移動計算機２は、本来、ホームネットワーク１１に接続されているが、現在は移動して、組織ネットワーク外のグローバルアドレスで運用されている箇所に接続されているとする。

【００３１】ホームネットワーク１１には、パケット中継装置５が設置される。このパケット中継装置５は、パケット暗号化の機能と、移動ＩＰのホームエージェントの機能（移動計算機の現在位置を管理し、移動計算機宛に送られてきたパケットをカプセル化して現在位置に転送する機能）とを持っている。

【００３２】組織ネットワーク１の出口すなわちインターネット６との境界部分には、境界ゲートウェイ４が設置される。この境界ゲートウェイ４は、２つのインタフェースを持ち、組織外のグローバルアドレス（インターネット側）と組織内のプライベートアドレスの両方を持つ。

【００３３】なお、本実施形態ではノード間のデータ転送に暗号化通信を用いるが、このノード間の暗号化通信には、ノード間で共有された該ノード間に固有の共通鍵を用いるものとする。この共通鍵は予めノード間で共有しておくか、あるいは必要時にノード間で鍵共有のための手続きを行う。

【００３４】以下では移動計算機２が移動先からホームネットワーク１１内のパケット中継装置５との間で移動登録に関するやり取りを行う場合とサーバ７と通信する場合を例にとりつつ本実施形態について詳しく説明する。

【００３５】移動計算機２側では、自身の接続している

現在位置に関する情報を図２に例示する制御パネルで設定する。ここで、Ｐｒｉｖａｔｅ Ａｄｄｒｅｓｓ Ｒｅｇｉｏｎは移動計算機２が同じプライベートアドレス体系で運営される組織ネット内で移動したことを、Ｇｌｏｂａｌ Ａｄｄｒｅｓｓ Ｒｅｇｉｏｎは組織ネット外部に出たことを示す。

【００３６】Ｇｌｏｂａｌ Ａｄｄｒｅｓｓ Ｒｅｇｉｏｎを選択した場合は、Ｂｏｒｄｅｒ Ｇａｔｅｗａｙ ＩＰ ａｄｄｒｅｓｓに境界ゲートウェイ４のグローバルアドレスを設定する（例えば、２０２，２４９，１０，１２２）。また、自身の現在位置のアドレスを設定する（この設定フィールドは図２においては省略してある）。

【００３７】なお、上記では、ユーザが陽に指定を行うようにしたが、例えばインターネットプロバイダーのサーバとＰＰＰで接続する際のネゴシエーションメッセージを基にこれらの情報を自動的に設定することも可能である。すなわち、一般にインターネットプロバイダと電話回線を通じてＰＰＰというプロトコルでＩＰ接続を行う場合、ＰＰＰプロトコルの初期セット時にＩＰＣＰというプロトコルで割り当てられるアドレスを決める。そのような場合、移動計算機２側では特定のアドレスを設定できないので、例えば図３のように、「アドレスをＩＳＰ側から自動的割り当てする」あるいは「アドレスを自動取得する」というような設定ボタンを設け、これを選択する。これを選択した場合、ＰＰＰのプロトコルの途上で獲得したＩＰアドレスがそのまま現在位置アドレスにセットされる。

【００３８】次に、図２に例示した制御パネルで（あるいは自動的に）現在位置が設定された場合の移動登録メッセージの送信動作を説明する。まず、プライベートネット内で移動した場合について説明する。

【００３９】移動計算機２は、組織内（例えば企業内）のプライベートネット内で移動した旨の情報がセットされると、通常の移動ＩＰの規定通り、ホームネットワーク１１のパケット中継装置５宛に、対応する鍵で登録要求パケットのペイロードを暗号化して送信する。

【００４０】暗号化された登録要求パケットを受信したパケット中継装置５では、送信元の移動計算機２に対応する鍵で該パケットを復号し、得られたパケットの内容を検査する。パケット・ヘッダ内の識別情報（例えばパケットタイプ・フィールドに記述されたコード）から移動ＩＰの登録要求であることが判ると、該パケットから該移動計算機２のホームアドレスと現在位置アドレスを取り出し、これを図５のような管理テーブルに登録する。また、送信先である移動計算機２に対応する鍵で、登録要求に対する応答パケット（登録成功パケット）のペイロードを暗号化して、これを移動計算機２宛てに返送する。

【００４１】なお、図５において、Ｈｏｍｅ－ａｄｄｒは移動計算機２のホームアドレスを、Ｃｕｒｒｅｎｔ－ａｄｄｒは移動計算機２の現在位置アドレスを、ＫｅｙｓはこのＨｏｍｅ－ａｄｄｒとＣｕｒｒｅｎｔ－ａｄｄｒの組を持つパケットを転送する際に暗号化や復号に用いる鍵であり、転送先ノードに対応して記憶される。

【００４２】暗号化された応答パケットを受信した移動計算機２では、送信元のパケット中継装置５に対応する鍵で該パケットを復号し、得られた応答パケットから、登録に成功したことを認識する。

【００４３】次に、組織外のグローバルネットに移動した場合について説明する。移動計算機２が組織外のグローバルネットに移動した旨の情報がセットされると、Ｂｏｒｄｅｒ Ｇａｔｅｗａｙ ＩＰ ａｄｄｒｅｓｓに設定されたアドレスを用いて、組織ネットワーク１の出口の境界ゲートウェイ４のグローバルアドレスインタフェース宛に、対応する鍵で暗号化した移動ＩＰの登録要求パケットを送信する。このパケット形式を図４（ａ）に示す。ハッチングされた部分は暗号化されている部分である（図４（ｂ）～（ｆ）も同様である）。

【００４４】境界ゲートウェイ４は、自分宛に暗号化パケットが送信されてくると、送信元を調べ、送信元（この場合、移動計算機２）に対応する鍵でこのパケットを復号し、得られたパケットの内容を検査する。パケット・ヘッダ内の識別情報（例えばパケットタイプ・フィールドに記述されたコード）から移動ＩＰの登録要求であることが判ると、該パケットから送信元の移動計算機２のホームアドレスと現在位置アドレスとを取り出し、これを図５のような管理テーブルに登録する。

【００４５】次に、境界ゲートウェイ４は、転送先であるホームネットワーク１１のパケット中継装置５に対応する鍵で該移動登録パケットを再暗号化し、これを該パケット中継装置５宛てに転送する。このパケット形式を図４（ｂ）に示す。

【００４６】ホームネットワーク１１のパケット中継装置５は、境界ゲートウェイ４からの中継／再暗号化された登録要求パケットを受け取ると、パケットヘッダから送信元を調べ、（暗号化パケットのヘッダにおける）送信元である境界ゲートウェイ４に対応する鍵でこのパケットを復号し、得られたパケットの内容を検査する。パケット・ヘッダ内の識別情報から移動ＩＰの登録要求であることが判ると、該パケットから送信元の移動計算機２のホームアドレスと現在位置アドレスとを取り出し、これを図５のような管理テーブルに登録する。

【００４７】また、パケット中継装置５は、移動計算機２に登録要求に対する応答パケット（登録成功パケット）を返送するために、次段ノード（中継ノード）となる境界ゲートウェイ４宛てに、これに対応する鍵で暗号化した該応答パケットを送信する。このパケット形式を図４（ｃ）に示す。

【００４８】境界ゲートウェイ４は、パケット中継装置

５からの暗号化パケットを受け取ると、送信元を調べ、送信元すなわちパケット中継装置５に対応する鍵でこのパケットを復号し、得られたパケットの内容を検査する。パケット・ヘッダ内の識別情報から移動ＩＰの応答パケットであることが判ると、パケット・ヘッダ内に記述された移動計算機２のホームアドレスと、図５の管理テーブルとから、移動計算機２の現在位置アドレスを求め、移動計算機２に対応する鍵で再暗号化した応答パケットを、この移動計算機２の現在位置アドレス宛てに転送する。このパケット形式を図４（ｄ）に示す。

【００４９】暗号化された応答パケットを受信した移動計算機２では、（暗号化パケットのヘッダにおける）送信元である境界ゲートウェイ４に対応する鍵で該パケットを復号し、得られた応答パケットから、登録に成功したことを認識する。

【００５０】以上のように、移動ＩＰの登録要求パケットが受諾されると、それ以降、移動計算機２のホームアドレス宛に送信されてきたパケットをホームネットワーク１１のパケット中継装置５が捕捉し、これを移動計算機２の現在位置アドレス宛パケット内にカプセル化し、さらにこれを境界ゲートウェイ２に対応する鍵で暗号化して、境界ゲートウェイ５のプライベートアドレス宛に転送する。このパケット形式を図４（ｅ）に示す。なお、図４（ｅ）ではデータグラム（Ｄａｔａｇｒａｍ）の部分に通信相手発で移動計算機２のホームドレス宛のパケットがカプセル化される。そして、境界ゲートウェイ５は前述した移動登録の応答と同様にこのパケットを中継し、移動計算機宛に再暗号化して転送する。このパケット形式を図４（ｆ）に示す。

【００５１】また、移動計算機２が通信相手のサーバ７にパケットを送信する場合も、サーバ７のアドレスがホームネットワーク１１のパケット中継装置５と同じポリシーで管理されるプライベートアドレスであるなら、前述の登録要求の場合と同様にして、移動計算機２は境界ゲートウェイ４との間で暗号化し、境界ゲートウェイ４のグローバルアドレス宛に送信する。そして、境界ゲートウェイ４は一度これを復号し、サーバ７宛のプライベートアドレスを用いた暗号化パケットに変換して転送する。

【００５２】このように、本実施形態に係る境界ゲートウェイ４により、グローバルネットワークとプライベートネットワークの境界で、２つの個別の暗号化転送路を構築することで、２つのアドレス空間を跨ぐ通信を可能とする。

【００５３】以上、本実施形態について説明してきたが、従来の移動ＩＰ方式では、移動計算機はホームネットワークとの到達可能性（ｒｅａｃｈａｂｉｌｉｔｙ）の保証された単一空間内でのみ移動が許されており、大規模な組織で組織内ネットワークをプライベートアドレスで構築している場合、組織外のグローバルアドレス領

域に移動した計算機からは移動ＩＰ方式をそのまま使用できなかったが、本実施形態によれば、移動計算機側で自身の現在位置に応じて適切な形式でパケットを生成、送信するような制御を可能とし、また、組織ネットワークの入口で移動計算機からのパケットを一旦受信し、内容を確認して、組織内の該当するホームエージェント（パケット中継装置）宛に転送する処理を行うことにより、企業ネット等の組織ネットがプライベートアドレスで運用しており、移動計算機が組織外のグローバルアドレスに移動しても移動ＩＰ方式をそのまま使用し続けることができる。

【００５４】一般に、大規模ネットワークでは、組織ネットの入口で通信内容のログを取ったりすることが多く、境界ゲートウェイの処理のオーバーヘッドは実際には問題にならない場合が多い。また、境界ゲートウェイでファイアウォールなどの他の制御機構を共存させる場合も拡張が容易である。

【００５５】また、本実施形態において、インターネットプロバイダなどに接続するシーケンス内で移動計算機のＩＰネットワーク上の位置を検出することで、移動計算機側の制御をさらに容易にできる。

【００５６】なお、本発明は、ＲＦＣ２００２に示される移動ＩＰだけでなく、他の様々な移動通信プロトコルに対しても適用可能である。また、以上の各機能は、ソフトウェアとしても実現可能である。また、上記した各手順あるいは手段をコンピュータに実行させるためのプログラムを記録した機械読取り可能な媒体として実施することもできる。本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【００５７】

【発明の効果】本発明によれば、移動計算機が本来属するホームネットワークとは異なるアドレス空間に移動した場合、移動計算機と境界ゲートウェイ等のパケット転送装置との間でそのアドレス空間におけるアドレスを用いて通信を行い、境界ゲートウェイ等のパケット転送装置とホームネットワーク内に位置するホームエージェント等のパケット転送装置やサーバ装置等のノードとの間でホームネットワークにおけるアドレスを用いて通信を行うので、移動計算機が組織外のグローバルアドレスに移動しても移動ＩＰ方式をそのまま使用し続けることができる。

【図面の簡単な説明】

【図１】本実施形態に係るネットワークの基本構成を示す図

【図２】制御パネルの一例を示す図

【図３】制御パネルの他の例を示す図

【図４】パケット形式の例を示す図

【図５】管理テーブルの一例を示す図

【図６】移動ＩＰ方式について説明するための図

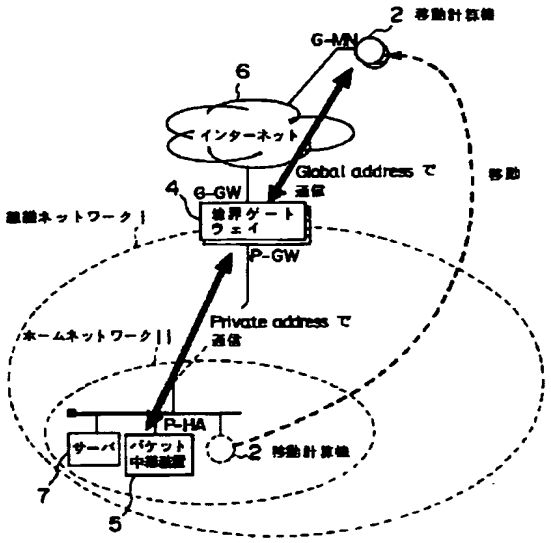
17

【符号の説明】
1…組織ネットワーク
2…移動計算機
5…パケット中継装置

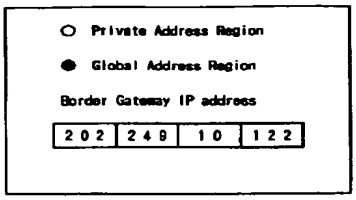
18

＊6…インターネット
4…境界ゲートウェイ
7…サーバ
＊　１１…ホームネットワーク

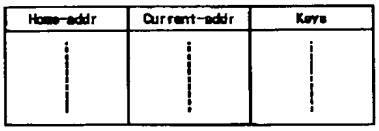
【図１】



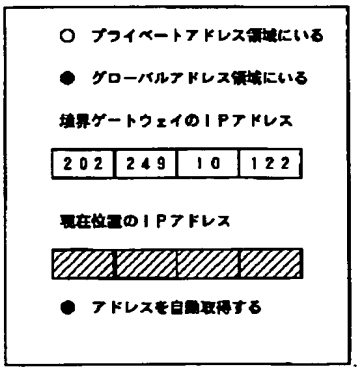
【図２】



【図５】

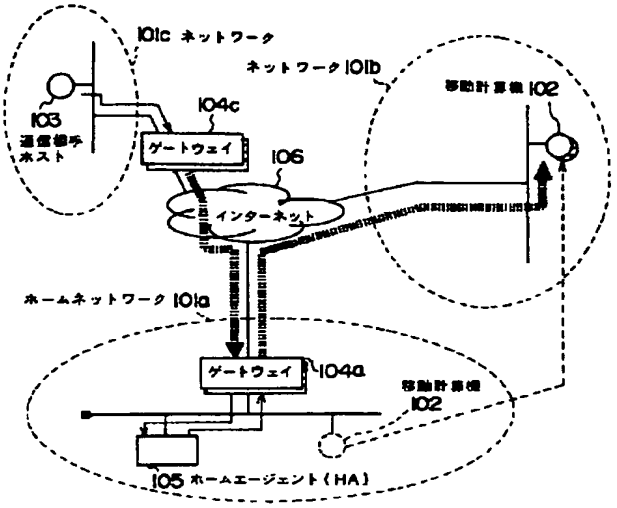


【図３】



【図４】

【図６】



【手続補正書】
【提出日】平成１０年１０月７日
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】全文
【補正方法】変更
【補正内容】
【書類名】　　明細書
【発明の名称】　　パケット中継装置、移動計算機装置、移動計算機管理装置、パケット中継方法、パケット送信方法及び移動計算機位置登録方法
【特許請求の範囲】
【請求項１】移動計算機がネットワーク間を移動して通信を行えるようにサポートするネットワークシステム中に設置され、移動計算機のアドレスが送信元もしくは宛先に付されたパケットを中継するパケット中継装置であって、
ホームネットワークとは異なるアドレス方式で管理される移動先ネットワークから、位置登録のために移動計算機が発したパケットであって、ホームネットワークとは異なるアドレスを用いる形式のものを受信する受信手段と、
受信した前記パケットの内容を検査し、この内容に基づいて、該パケットを、プライベートアドレス形式で管理される、移動計算機のホームネットワークに設置された通信相手の計算機へ、プライベートアドレスを用いる形式として転送する転送手段とを具備することを特徴とするパケット中継装置。
【請求項２】前記受信手段は、受信した前記パケットを、前記移動計算機との間で使用される鍵を用いて復号する手段を含み、
前記転送手段は、復号されたパケットを、前記通信相手の計算機との間で使用される鍵を用いて再度暗号化し、暗号化されたパケットに、送信元を自装置のプライベートアドレスとし、宛先を前記通信相手のプライベートアドレスとするヘッダを付加する手段を含むことを特徴とする請求項１に記載のパケット中継装置。
【請求項３】自装置のプライベートアドレスと、ホームネットワークとは異なるアドレスとしてグローバルアドレスとを記憶する第１の記憶手段と、
前記移動計算機の、移動先ネットワークにおける現在位置アドレス、ホームネットワークにおけるホームアドレス、及び前記移動計算機との間での暗号化に使用される鍵を記憶する第２の記憶手段とを更に具備することを特徴とする請求項１に記載のパケット中継装置。
【請求項４】前記通信相手の計算機が、前記移動計算機宛のパケットを該移動計算機の現在位置アドレス宛に転送する手段を有する移動計算機管理装置であり、受信した前記パケットが該現在位置アドレスの情報を含む位置登録要求パケットである場合に、該現在位置アドレスを前記第２の記憶手段に登録する手段を更に具備することを特徴とする請求項３に記載のパケット中継装置。
【請求項５】前記受信手段は、前記通信相手の計算機から、プライベートアドレスを用いる形式の別のパケットを受信する手段を含み、
前記転送手段は、受信した前記別のパケットの内容を検査し、この内容に基づいて、該別のパケットを、移動先

ネットワークの前記移動計算機へ、ホームネットワークとは異なるアドレスを用いる形式として転送する手段を含むことを特徴とする請求項１に記載のパケット中継装置。

【請求項６】前記受信手段は、受信した前記別のパケットを、前記通信相手の計算機との間で使用される鍵を用いて復号する手段を含み、

前記転送手段は、復号されたパケットを、前記移動計算機との間で使用される鍵を用いて再度暗号化し、暗号化されたパケットに、送信元を自装置のグローバルアドレスとし、宛先を前記移動計算機のグローバルアドレスとするヘッダを付加する手段を含むことを特徴とする請求項５に記載のパケット中継装置。

【請求項７】相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、

自装置宛のパケットを自装置の現在位置アドレス宛に転送する手段を有する移動計算機管理装置の設置されたホームネットワークと同じプライベートアドレス空間に自装置が接続されているか否かを示す情報を記憶する第１の記憶手段と、

前記ホームネットワークのプライベートアドレス空間と、これとは異なるアドレス空間との境界に設置され、該プライベートアドレス空間に接続された計算機と該異なるアドレス空間に接続された計算機との間で送受信されるパケットを中継する手段を有するパケット中継装置の、該異なるアドレス空間におけるアドレスを記憶する第２の記憶手段と、

前記第１の記憶手段に記憶された情報が、自装置が前記ホームネットワークとは異なるアドレス空間に接続されていることを示している場合に、現在位置アドレス情報を含む前記移動計算機管理装置宛の位置登録要求パケットを、前記第２の記憶手段に記憶された前記パケット中継装置の異なるアドレス空間におけるアドレスを用いて、送信する送信手段とを具備することを特徴とする移動計算機装置。

【請求項８】前記送信手段は、前記第１の記憶手段に記憶された情報が、自装置が前記ホームネットワークとは異なるアドレス空間に接続されていることを示している場合に、前記ホームネットワークに設置された通信相手の計算機を宛先とする全パケットを暗号化して、前記第２の記憶手段に記憶された前記パケット中継装置の異なるアドレス空間におけるアドレスを用いて、送信する手段を含むことを特徴とする請求項７に記載の移動計算機装置。

【請求項９】移動先ネットワークにおけるアドレスを自動取得するか否かを設定する手段と、

前記第１の記憶手段に記憶された情報が、自装置が前記ホームネットワークとは異なるアドレス空間に接続されていることを示している場合に、前記自動取得することを示す設定がされているならば、該異なるアドレス空間におけるアドレスの割り当てを受けるべく所定のプロトコルを実行して取得したアドレスを自装置の現在位置アドレスとする手段とを更に具備することを特徴とする請求項７に記載の移動計算機管理装置。

【請求項１０】移動計算機がネットワーク間を移動して通信を行えるように、該移動計算機のホームネットワーク内に設置され、該移動計算機宛のパケットを該移動計算機の現在位置アドレス宛に転送する手段を有する移動計算機管理装置であって、

前記ホームネットワークにおける各移動計算機のホームアドレス情報と、各移動計算機がホームネットワーク外に移動した場合の現在位置アドレス情報とを対応付けて記憶する記憶手段と、

前記ホームネットワークのプライベートアドレス空間と、これとは異なるアドレス空間との境界に設置され、該プライベートアドレス空間に接続された計算機と該異なるアドレス空間に接続された計算機との間で送受信されるパケットを中継する手段を有するパケット中継装置から中継されてきた暗号化パケットを復号し、得られたパケットが自装置の管理対象である移動計算機から自装置宛に発せられた、現在位置アドレス情報を含む位置登録パケットである場合に、該現在位置アドレス情報を前記記憶手段に登録する手段とを具備することを特徴とする移動計算機管理装置。

【請求項１１】前記位置登録パケットに対する前記移動計算機宛の登録応答パケットを、前記パケット中継装置宛に暗号化して送信する手段を更に具備することを特徴とする請求項１０に記載の移動計算機管理装置。

【請求項１２】前記ホームネットワーク外に移動中の移動計算機のホームアドレス宛に転送されてきたパケットを捕捉した場合、該パケットを、送信元を自装置のアドレス、宛先を該移動計算機の現在位置アドレスとするパケットにカプセル化し、このカプセル化されたパケットを暗号化して、前記パケット中継装置の前記プライベートアドレス空間におけるアドレスを用いて、送信する手段を更に具備することを特徴とする請求項１０に記載の移動計算機管理装置。

【請求項１３】移動計算機がネットワーク間を移動して通信を行えるようにサポートするネットワークシステム中に設置され、移動計算機のアドレスが送信元もしくは宛先に付されたパケットを中継するパケット中継装置のパケット中継方法であって、

ホームネットワークとは異なるアドレス方式で管理される移動先ネットワークから、位置登録のために移動計算機が発したパケットであって、ホームネットワークとは異なるアドレスを用いる形式のものを受信し、

受信した前記パケットの内容を検査し、この内容に基づいて、該パケットを、プライベートアドレス形式で管理される、移動計算機のホームネットワークに設置された通信相手の計算機へ、プライベートアドレスを用いる形

式として転送することを特徴とするパケット中継方法。
【請求項１４】相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置のパケット送信方法であって、
自装置宛のパケットを自装置の現在位置アドレス宛に転送する手段を有する移動計算機管理装置の設置されたホームネットワークと同じプライベートアドレス空間に自装置が接続されているか否かを示す情報を得て、これを第１の記憶手段に記憶し、該ホームネットワークのプライベートアドレス空間と、これとは異なるアドレス空間との境界に設置され、該プライベートアドレス空間に接続された計算機と該異なるアドレス空間に接続された計算機との間で送受信されるパケットを中継する手段を有するパケット中継装置の、該異なるアドレス空間におけるアドレスを得た場合に、これを第２の記憶手段に記憶し、
前記第１の記憶手段に記憶された情報が、自装置が前記ホームネットワークとは異なるアドレス空間に接続されていることを示している場合に、現在位置アドレス情報を含む前記移動計算機管理装置宛の位置登録要求パケットを、前記第２の記憶手段に記憶された前記パケット中継装置の異なるアドレス空間におけるアドレスを用いて、送信することを特徴とするパケット送信方法。
【請求項１５】移動計算機がネットワーク間を移動して通信を行えるように、該移動計算機のホームネットワーク内に設置され、該移動計算機宛のパケットを該移動計算機の現在位置アドレス宛に転送する手段を有する移動計算機管理装置の移動計算機位置登録方法であって、
前記ホームネットワークのプライベートアドレス空間と、これとは異なるアドレス空間との境界に設置され、該プライベートアドレス空間に接続された計算機と該異なるアドレス空間に接続された計算機との間で送受信されるパケットを中継する手段を有するパケット中継装置から中継されてきた暗号化パケットを復号し、
得られたパケットが自装置の管理対象である移動計算機から自装置宛に発せられた、現在位置アドレス情報を含む位置登録パケットである場合に、該現在位置アドレス情報を該移動計算機のホームアドレス情報に対応付けて記憶することを特徴とする移動計算機位置登録方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、相互接続している複数のネットワーク上を移動しながら通信を行う移動計算機及びその移動計算機を宛先または送信元とするデータパケットを中継するパケット中継装置並びにパケット中継方法、パケット送信方法及び移動計算機登録方法に関する。
【０００２】
【従来の技術】計算機システムの小型化、低価格化やネットワーク環境の充実に伴って、計算機システムの利用は急速にかつ種々の分野に広く拡大し、また集中型システムから分散型システムへの移行が進んでいる。特に近年では計算機システム自体の進歩、能力向上に加え、コンピュータ・ネットワーク技術の発達・普及により、オフィス内のファイルやプリンタなどの資源共有のみならず、オフィス外、一組織外とのコミュニケーション（電子メール、電子ニュース、ファイルの転送など）が可能になり、これらが広く利用されはじめた。特に近年では、世界最大のコンピュータネットワーク「インターネット（ｉｎｔｅｒｎｅｔ）」の利用が普及しており、インターネットと接続し、公開された情報、サービスを利用したり、逆にインターネットを通してアクセスしてくる外部ユーザに対し、情報、サービスを提供することで、新たなコンピュータビジネスが開拓されている。また、インターネット利用に関して、新たな技術開発、展開がなされている。
【０００３】また、このようなネットワークの普及に伴い、移動通信（ｍｏｂｉｌｅ　ｃｏｍｐｕｔｉｎｇ）に対する技術開発も行われている。移動通信では、携帯型の端末、計算機を持ったユーザがネットワーク上を移動して通信する。ときには通信を行いながらネットワーク上の位置を変えていく場合もあり、そのような通信において変化する移動計算機のネットワーク上のアドレスを管理し、正しく通信内容を到達させるための方式が必要である。
【０００４】一般に移動通信を行う場合、移動計算機が所属していたネットワークに移動計算機の移動先データを管理するルータ（ホームエージェント）を置き、移動計算機が移動した場合、このホームエージェントに対して現在位置を示す登録メッセージを送る。登録メッセージが受け取られたら、移動計算機宛データの送信はそのホームエージェントを経由して、移動計算機の元のアドレス宛のＩＰパケットを移動計算機の現在位置アドレス宛パケット内にカプセル化することで移動計算機に対するデータの経路制御が行われる。例えば、図６では、元々ホームネットワーク１０１ａに属していた移動計算機１０２が、他のネットワーク１０１ｂに移動し、ネットワーク１０１ｃ内の他の計算機（ＣＨ）１０３との間で通信を行う場合に、移動計算機１０２に対しホームエージェント（ＨＡ）１０５が上記の役割を行う。この方式は、インターネットの標準化団体であるＩＥＴＦのｍｏｂｉｌｅ－ＩＰワーキンググループで標準化が進められている移動ＩＰと呼ばれる方式である（文献：ＲＦＣ２００２，　ＩＰ　ｍｏｂｉｌｉｔｙ　ｓｕｐｐｏｒｔ（Ｃ．Ｐｅｒｋｉｎｓ））。
【０００５】また、ネットワークが普及し、ネット間の自由な接続が実現され、膨大なデータ、サービスのやりとりがなされる場合、セキュリティ上の問題を考慮する必要が生じてくる。例えば組織内部の秘密情報の外部ネットワークへの漏洩をいかに防ぐか、という問題や、組

織外からの不正な侵入から、組織内ネットワークに接続された資源、情報をいかに守るか、という問題である。インターネットは、当初学術研究を目的に構築されたため、ネットワークの接続による自由なデータサービスのやりとりを重視しており、このようなセキュリティ上の問題は考慮されていなかったが、近年多くの企業、団体がインターネットに接続するようになり、セキュリティ上の問題から自組織ネットワークを防衛する機構が必要となってきた。

【０００６】そこで、インターネット上でデータパケットを交換する際に、外部にデータパケットを送出する前にその内容を暗号化し認証コードをつけ、受信したサイトで認証コードを確認し復号化する、という方法がある。この方法によれば、たとえ組織外のユーザが外部ネットワーク上のデータパケットを取り出しても、内容が暗号化されているので、決してその内部が漏洩することがなく、安全な通信が確保できる。

【０００７】このような暗号化通信をサポートするゲートウェイ計算機で守られた（ガードされた）ネットワーク同士であれば相互に暗号化通信が可能であり、また前述の移動計算機が自分でパケットの暗号化、復号を行う機能をサポートしていれば、任意のゲートウェイ間、またはゲートウェイ～移動計算機間で暗号化通信がサポートできる。例えば図６では、元々ホームネットワーク１０１ａに属していた移動計算機１０２が、他のネットワーク１０１ｂに移動し、ネットワーク１０１ｃ内の他の計算機（ＣＨ）１０３と暗号化、復号機能をサポートするゲートウェイ１０４ａ，１０４ｃを介して暗号化通信を行う。

【０００８】図６では、移動ＩＰとパケット暗号化を併用して通信を行う場合、パケットの転送経路は、

ＣＨ→ゲートウェイ１０４ｃ→ゲートウェイ１０４ａ→ホームエージェント（ＨＡ）１０５→ゲートウェイ１０４ａ→移動計算機１０２

となり、ゲートウェイ１０４ａでは、一旦パケットは復号されてホームエージェント１０５に送られ、その後、再度ホームエージェント１０５発のパケットが暗号化される。

【０００９】さて、移動ＩＰ方式では、単一のアドレス空間上を移動計算機が移動する場合のみを想定して、プロトコルが構成されている。すなわち、移動先からの現在位置の登録メッセージは必ずホームネットのホームエージェントに到達可能であると仮定している。しかし、昨今では大規模な組織がインターネットに接続する場合、ＩＰアドレスの枯渇の問題から、組織内の全てのホストにグローバルＩＰアドレスが割り当てられているのは稀で、組織内はプライベートアドレス（文献：ＲＦＣ１５９７）で運用し、外部に通信する場合は、グローバルアドレスへのアドレス変換を行う場合が多い。

【００１０】その場合、グローバルアドレス領域に移動した移動計算機から、プライベートアドレス領域内のホームエージェントに送信された登録要求パケットは、そのままでは到達可能でない。

【００１１】

【発明が解決しようとする課題】従来の移動ＩＰ方式では、移動計算機はホームネットワークとの到達可能性（ｒｅａｃｈａｂｉｌｉｔｙ）を仮定してプロトコルを構成していたため、ホームネットワークと共通のアドレス空間内のみを移動するという制約があった。このため、組織がプライベートアドレスで運用された場合、移動計算機が組織ネットワークの外（グローバルアドレス領域）に移動すると、移動ＩＰ方式がそのまま使用できないという欠点があった。

【００１２】本発明は、上記事情を考慮してなされたもので、複数の計算機が複数の相互接続された通信ネットワークにより互いに接続されて相互に通信可能に構成された計算機システムで、移動ＩＰによる移動計算機への自動経路制御がサポートされている場合において、ホームネットワークと異なるアドレス管理領域に移動した移動計算機発の位置登録メッセージなどのパケットの適切な処理を可能とするパケット中継装置、移動計算機装置、移動計算機管理装置、パケット中継方法、パケット送信方法及び移動計算機位置登録方法を提供することを目的とする。

【００１３】

【課題を解決するための手段】本発明（請求項１）は、移動計算機がネットワーク間を移動して通信を行えるようにサポートするネットワークシステム中に設置され、移動計算機のアドレスが送信元もしくは宛先に付されたパケットを中継するパケット中継装置であって、ホームネットワークとは異なるアドレス（例えばグローバルアドレス）方式で管理される移動先ネットワークから、位置登録のために移動計算機が発したパケットであって、ホームネットワークとは異なるアドレスを用いる形式のものを受信する受信手段と、受信した前記パケットの内容を検査し、この内容に基づいて、該パケットを、プライベートアドレス形式で管理される、移動計算機のホームネットワークに設置された通信相手の計算機へ、プライベートアドレスを用いる形式として転送する転送手段とを具備することを特徴とする。

【００１４】なお、発明の実施の形態においては、パケット中継装置を「境界ゲートウェイ」と呼ぶことがある。好ましくは、前記受信手段は、受信した前記パケットを、前記移動計算機との間で使用される鍵を用いて復号する手段を含み、前記転送手段は、復号されたパケットを、前記通信相手の計算機との間で使用される鍵を用いて再度暗号化し、暗号化されたパケットに、送信元を自装置のプライベートアドレスとし、宛先を前記通信相手のプライベートアドレスとするヘッダを付加する手段を含むようにしてもよい。

【００１５】このましくは、自装置のプライベートアドレスと、ホームネットワークとは異なるアドレスとしてグローバルアドレスとを記憶する第１の記憶手段と、前記移動計算機の、移動先ネットワークにおける現在位置アドレス、ホームネットワークにおけるホームアドレス、及び前記移動計算機との間での暗号化に使用される鍵を記憶する第２の記憶手段とを更に具備するようにしてもよい。

【００１６】好ましくは、前記通信相手の計算機が、前記移動計算機宛のパケットを該移動計算機の現在位置アドレス宛に転送する手段を有する移動計算機管理装置であり、受信した前記パケットが該現在位置アドレスの情報を含む位置登録要求パケットである場合に、該現在位置アドレスを前記第２の記憶手段に登録する手段を更に具備するようにしてもよい。

【００１７】好ましくは、前記受信手段は、前記通信相手の計算機から、プライベートアドレスを用いる形式の別のパケットを受信する手段を含み、前記転送手段は、受信した前記別のパケットの内容を検査し、この内容に基づいて、該別のパケットを、移動先ネットワークの前記移動計算機へ、ホームネットワークとは異なるアドレスを用いる形式として転送する手段を含むようにしてもよい。

【００１８】好ましくは、前記受信手段は、受信した前記別のパケットを、前記通信相手の計算機との間で使用される鍵を用いて復号する手段を含み、前記転送手段は、復号されたパケットを、前記移動計算機との間で使用される鍵を用いて再度暗号化し、暗号化されたパケットに、送信元を自装置のグローバルアドレスとし、宛先を前記移動計算機のグローバルアドレスとするヘッダを付加する手段を含むようにしてもよい。

【００１９】本発明（請求項７）は、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、自装置宛のパケットを自装置の現在位置アドレス宛に転送する手段を有する移動計算機管理装置の設置されたホームネットワークと同じプライベートアドレス空間に自装置が接続されているか否かを示す情報を記憶する第１の記憶手段と、前記ホームネットワークのプライベートアドレス空間と、これとは異なるアドレス空間との境界に設置され、該プライベートアドレス空間に接続された計算機と該異なるアドレス空間に接続された計算機との間で送受信されるパケットを中継する手段を有するパケット中継装置の、該異なるアドレス空間におけるアドレスを記憶する第２の記憶手段と、前記第１の記憶手段に記憶された情報が、自装置が前記ホームネットワークとは異なるアドレス空間に接続されていることを示している場合に、現在位置アドレス情報を含む前記移動計算機管理装置宛の位置登録要求パケットを、前記第２の記憶手段に記憶された前記パケット中継装置の異なるアドレス空間におけるアドレスを用いて、送信する送信手段とを具備することを特徴とする。

【００２０】好ましくは、前記送信手段は、前記第１の記憶手段に記憶された情報が、自装置が前記ホームネットワークとは異なるアドレス空間に接続されていることを示している場合に、前記ホームネットワークに設置された通信相手の計算機を宛先とする全パケットを暗号化して、前記第２の記憶手段に記憶された前記パケット中継装置の異なるアドレス空間におけるアドレスを用いて、送信する手段を含むようにしてもよい。

【００２１】好ましくは、移動先ネットワークにおけるアドレスを自動取得するか否かを設定する手段と、前記第１の記憶手段に記憶された情報が、自装置が前記ホームネットワークとは異なるアドレス空間に接続されていることを示している場合に、前記自動取得することを示す設定がされているならば、該異なるアドレス空間におけるアドレスの割り当てを受けるべく所定のプロトコルを実行して取得したアドレスを自装置の現在位置アドレスとする手段とを更に具備するようにしてもよい。

【００２２】本発明（請求項１０）は、移動計算機がネットワーク間を移動して通信を行えるように、該移動計算機のホームネットワーク内に設置され、該移動計算機宛のパケットを該移動計算機の現在位置アドレス宛に転送する手段を有する移動計算機管理装置であって、前記ホームネットワークにおける各移動計算機のホームアドレス情報と、各移動計算機がホームネットワーク外に移動した場合の現在位置アドレス情報とを対応付けて記憶する記憶手段と、前記ホームネットワークのプライベートアドレス空間と、これとは異なるアドレス空間との境界に設置され、該プライベートアドレス空間に接続された計算機と該異なるアドレス空間に接続された計算機との間で送受信されるパケットを中継する手段を有するパケット中継装置から中継されてきた暗号化パケットを復号し、得られたパケットが自装置の管理対象である移動計算機から自装置宛に発せられた、現在位置アドレス情報を含む位置登録パケットである場合に、該現在位置アドレス情報を前記記憶手段に登録する手段とを具備することを特徴とする。

【００２３】なお、発明の実施の形態においては、移動計算機管理装置を「パケット中継装置」もしくは「ホームエージェント」と呼ぶことがある。好ましくは、前記位置登録パケットに対する前記移動計算機宛の登録応答パケットを、前記パケット中継装置宛に暗号化して送信する手段を更に具備するようにしてもよい。

【００２４】好ましくは、前記ホームネットワーク外に移動中の移動計算機のホームアドレス宛に転送されてきたパケットを捕捉した場合、該パケットを、送信元を自装置のアドレス、宛先を該移動計算機の現在位置アドレスとするパケットにカプセル化し、このカプセル化されたパケットを暗号化して、前記パケット中継装置の前記プライベートアドレス空間におけるアドレスを用いて、

送信する手段を更に具備するようにしてもよい。

【００２５】本発明（請求項１３）は、移動計算機がネットワーク間を移動して通信を行えるようにサポートするネットワークシステム中に設置され、移動計算機のアドレスが送信元もしくは宛先に付されたパケットを中継するパケット中継装置のパケット中継方法であって、ホームネットワークとは異なるアドレス（例えばグローバルアドレス）方式で管理される移動先ネットワークから、位置登録のために移動計算機が発したパケットであって、ホームネットワークとは異なるアドレスを用いる形式のものを受信し、受信した前記パケットの内容を検査し、この内容に基づいて、該パケットを、プライベートアドレス形式で管理される、移動計算機のホームネットワークに設置された通信相手の計算機へ、プライベートアドレスを用いる形式として転送することを特徴とする。

【００２６】本発明（請求項１４）は、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置のパケット送信方法であって、自装置宛のパケットを自装置の現在位置アドレス宛に転送する手段を有する移動計算機管理装置の設置されたホームネットワークと同じプライベートアドレス空間に自装置が接続されているか否かを示す情報を得て、これを第１の記憶手段に記憶し、該ホームネットワークのプライベートアドレス空間と、これとは異なるアドレス空間との境界に設置され、該プライベートアドレス空間に接続された計算機と該異なるアドレス空間に接続された計算機との間で送受信されるパケットを中継する手段を有するパケット中継装置の、該異なるアドレス空間におけるアドレスを得た場合に、これを第２の記憶手段に記憶し、前記第１の記憶手段に記憶された情報が、自装置が前記ホームネットワークとは異なるアドレス空間に接続されていることを示している場合に、現在位置アドレス情報を含む前記移動計算機管理装置宛の位置登録要求パケットを、前記第２の記憶手段に記憶された前記パケット中継装置の異なるアドレス空間におけるアドレスを用いて、送信することを特徴とする。

【００２７】なお、第１の記憶手段への記憶と第２の記憶手段への記憶については、第１の記憶手段への記憶が先に行われる場合と、第２の記憶手段への記憶が先に行われる場合とがあり得、上記の記載はその両方の場合を含む意味である。

【００２８】本発明（請求項１５）は、移動計算機がネットワーク間を移動して通信を行えるように、該移動計算機のホームネットワーク内に設置され、該移動計算機宛のパケットを該移動計算機の現在位置アドレス宛に転送する手段を有する移動計算機管理装置の移動計算機位置登録方法であって、前記ホームネットワークのプライベートアドレス空間と、これとは異なるアドレス空間との境界に設置され、該プライベートアドレス空間に接続された計算機と該異なるアドレス空間に接続された計算機との間で送受信されるパケットを中継する手段を有するパケット中継装置から中継されてきた暗号化パケットを復号し、得られたパケットが自装置の管理対象である移動計算機から自装置宛に発せられた、現在位置アドレス情報を含む位置登録パケットである場合に、該現在位置アドレス情報を該移動計算機のホームアドレス情報に対応付けて記憶することを特徴とする。

【００２９】なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【００３０】従来、移動ＩＰ方式では、移動計算機はホームネットワークとの到達可能性（ｒｅａｃｈａｂｉｌｉｔｙ）の保証された単一空間内でのみ移動が許されており、例えば大規模な組織で組織内ネットワークをプライベートアドレスで構築している場合、組織外のグローバルアドレス領域に移動した計算機からは移動ＩＰ方式をそのまま使用できなかった。これに対して本発明によれば、複数のアドレス空間が混在するネットワーク構成において、移動計算機側で自身の現在位置（プライベートアドレス領域で移動しているのか、組織外アドレス領域に移動したか）に応じて適切な形式で登録要求パケットを生成、送信するような制御を可能とし、また、組織ネットワークの入口で移動計算機から送信された登録要求パケットを一旦受信し、内容を確認して、組織内の該当する移動計算機管理装置（パケット中継装置、ホームエージェント）宛に転送する処理を行う（移動ＩＰ方式では、ホームエージェントはサブネットに１つ設置され、組織内に複数のホームエージェントが置かれる可能性もあるため）ことにより、例えば企業ネットがプライベートアドレスで運用しており、移動計算機が組織外のグローバルアドレスに移動しても移動ＩＰ方式をそのまま使用し続けることができる。

【００３１】一般に、大規模ネットワークでは、企業ネットの入口で通信内容のログを取ったりすることが多く、パケット中継装置（境界ゲートウェイ）の処理のオーバーヘッドは実際には問題にならない場合が多い。また、パケット中継装置（境界ゲートウェイ）でファイアウォールなどの他の制御機構を共存させる場合も拡張が容易である。

【００３２】また、本発明において、インターネットプロバイダなどに接続するシーケンス内で移動計算機のＩＰネットワーク上の位置を検出することで、移動計算機側の制御をさらに容易にできる。

【００３３】
【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。図１に、本実施形態に係るネットワークの基本構成を示す。図１では、組織ネットワーク１の中にホームネットワーク１１が存在する。組織ネットワーク（例えば企業内ネットワーク）１全体はプライベートアドレスで運用されている。移動計算機２は、本来、ホームネットワーク１１に接続されているが、現在は移動して、組織ネットワーク外のグローバルアドレスで運用されている箇所に接続されているとする。
【００３４】ホームネットワーク１１には、パケット中継装置（移動計算機管理装置）５が設置される。このパケット中継装置（移動計算機管理装置）５は、パケット暗号化の機能と、移動ＩＰのホームエージェントの機能（移動計算機の現在位置を管理し、移動計算機宛に送られてきたパケットをカプセル化して現在位置に転送する機能）とを持っている。
【００３５】組織ネットワーク１の出口すなわちインターネット６との境界部分には、境界ゲートウェイ４が設置される。この境界ゲートウェイ４は、２つのインタフェースを持ち、組織外のグローバルアドレス（インターネット側）と組織内のプライベートアドレスの両方を持つ。
【００３６】なお、本実施形態ではノード間のデータ転送に暗号化通信を用いるが、このノード間の暗号化通信には、ノード間で共有された該ノード間に固有の共通鍵を用いるものとする。この共通鍵は予めノード間で共有しておくか、あるいは必要時にノード間で鍵共有のための手続きを行う。
【００３７】以下では移動計算機２が移動先からホームネットワーク１１内のパケット中継装置（移動計算機管理装置）５との間で位置登録に関するやり取りを行う場合とサーバ７と通信する場合を例にとりつつ本実施形態について詳しく説明する。
【００３８】移動計算機２側では、自身の接続している現在位置に関する情報を図２に例示する制御パネルで設定する。ここで、Ｐｒｉｖａｔｅ　Ａｄｄｒｅｓｓ　Ｒｅｇｉｏｎは移動計算機２が同じプライベートアドレス体系で運営される組織ネット内で移動したことを、Ｇｌｏｂａｌ　Ａｄｄｒｅｓｓ　Ｒｅｇｉｏｎは組織ネット外部に出たことを示す。
【００３９】Ｇｌｏｂａｌ　Ａｄｄｒｅｓｓ　Ｒｅｇｉｏｎを選択した場合は、Ｂｏｒｄｅｒ　Ｇａｔｅｗａｙ　ＩＰ　ａｄｄｒｅｓｓに境界ゲートウェイ４のグローバルアドレスを設定する（例えば、２０２，２４９，１０，１２２）。また、自身の現在位置のアドレスを設定する（この設定フィールドは図２においては省略してある）。
【００４０】なお、上記では、ユーザが陽に設定を行うようにしたが、例えばインターネットプロバイダーのサーバとＰＰＰで接続する際のネゴシエーションメッセージを基にこれらの情報を自動的に設定することも可能である。すなわち、一般にインターネットプロバイダと電話回線を通じてＰＰＰというプロトコルでＩＰ接続を行う場合、ＰＰＰプロトコルの初期セット時にＩＰＣＰというプロトコルで割り当てられるアドレスを決める。そのような場合、移動計算機２側では特定のアドレスを設定できないので、例えば図３のように、「アドレスをＩＳＰ側から自動的割り当てする」あるいは「アドレスを自動取得する」というような設定ボタンを設け、これを選択する。これを選択した場合、ＰＰＰのプロトコルの途上で獲得したＩＰアドレスがそのまま現在位置アドレスにセットされる。
【００４１】次に、図２に例示した制御パネルで（あるいは自動的に）現在位置が設定された場合の位置登録メッセージの送信動作を説明する。まず、プライベートネット内で移動した場合について説明する。
【００４２】移動計算機２は、組織内（例えば企業内）のプライベートネット内で移動した旨の情報がセットされると、通常の移動ＩＰの規定通り、ホームネットワーク１１のパケット中継装置（移動計算機管理装置）５宛に、対応する鍵で登録要求パケットのペイロードを暗号化して送信する。
【００４３】暗号化された登録要求パケットを受信したパケット中継装置（移動計算機管理装置）５では、送信元の移動計算機２に対応する鍵で該パケットを復号し、得られたパケットの内容を検査する。パケット・ヘッダ内の識別情報（例えばパケットタイプ・フィールドに記述されたコード）から移動ＩＰの登録要求であることが判ると、該パケットから該移動計算機２のホームアドレスと現在位置アドレスを取り出し、これを図５のような管理テーブルに登録する。また、送信先である移動計算機２に対応する鍵で、登録要求に対する応答パケット（登録成功パケット）のペイロードを暗号化して、これを移動計算機２宛てに返送する。
【００４４】なお、図５において、Ｈｏｍｅ－ａｄｄｒは移動計算機２のホームアドレス、Ｃｕｒｒｅｎｔ－ａｄｄｒは移動計算機２の現在位置アドレス、Ｋｅｙｓはこのホーム－ａｄｄｒとＣｕｒｒｅｎｔ－ａｄｄｒの組を持つパケットを転送する際に暗号化や復号に用いる鍵であり、転送先ノードに対応して記憶される。
【００４５】暗号化された応答パケットを受信した移動計算機２では、送信元のパケット中継装置（移動計算機管理装置）５に対応する鍵で該パケットを復号し、得られた応答パケットから、登録に成功したことを認識する。
【００４６】次に、組織外のグローバルネットに移動した場合について説明する。移動計算機２が組織外のグローバルネットに移動した旨の情報がセットされると、Ｂｏｒｄｅｒ　Ｇａｔｅｗａｙ　ＩＰ　ａｄｄｒｅｓｓに

設定されたアドレスを用いて、組織ネットワーク１の出口の境界ゲートウェイ４のグローバルアドレスインタフェース宛に、対応する鍵で暗号化した移動ＩＰの登録要求パケットを送信する。このパケット形式を図４（ａ）に示す。ハッチングされた部分は暗号化されている部分である（図４（ｂ）～（ｆ）も同様である）。

【００４７】境界ゲートウェイ４は、自分宛に暗号化パケットが送信されてくると、送信元を調べ、送信元（この場合、移動計算機２）に対応する鍵でこのパケットを復号し、得られたパケットの内容を検査する。パケット・ヘッダ内の識別情報（例えばパケットタイプ・フィールドに記述されたコード）から移動ＩＰの登録要求であることが判ると、該パケットから送信元の移動計算機２のホームアドレスと現在位置アドレスとを取り出し、これを図５のような管理テーブルに登録する。

【００４８】次に、境界ゲートウェイ４は、転送先であるホームネットワーク１１のパケット中継装置（移動計算機管理装置）５に対応する鍵で該位置登録パケットを再暗号化し、これを該パケット中継装置（移動計算機管理装置）５宛てに転送する。このパケット形式を図４（ｂ）に示す。

【００４９】ホームネットワーク１１のパケット中継装置（移動計算機管理装置）５は、境界ゲートウェイ４からの中継／再暗号化された登録要求パケットを受け取ると、パケットヘッダから送信元を調べ、（暗号化パケットのヘッダにおける）送信元である境界ゲートウェイ４に対応する鍵でこのパケットを復号し、得られたパケットの内容を検査する。パケット・ヘッダ内の識別情報から移動ＩＰの登録要求であることが判ると、該パケットから送信元の移動計算機２のホームアドレスと現在位置アドレスとを取り出し、これを図５のような管理テーブルに登録する。

【００５０】また、パケット中継装置（移動計算機管理装置）５は、移動計算機２に登録要求に対する応答パケット（登録成功パケット）を返送するために、次段ノード（中継ノード）となる境界ゲートウェイ４宛てに、これに対応する鍵で暗号化した該応答パケットを送信する。このパケット形式を図４（ｃ）に示す。

【００５１】境界ゲートウェイ４は、パケット中継装置（移動計算機管理装置）５からの暗号化パケットを受け取ると、送信元を調べ、送信元すなわちパケット中継装置（移動計算機管理装置）５に対応する鍵でこのパケットを復号し、得られたパケットの内容を検査する。パケット・ヘッダ内の識別情報から移動ＩＰの応答パケットであることが判ると、パケット・ヘッダ内に記述された移動計算機２のホームアドレスと、図５の管理テーブルとから、移動計算機２の現在位置アドレスを求め、移動計算機２に対応する鍵で再暗号化した応答パケットを、この移動計算機２の現在位置アドレス宛てに転送する。このパケット形式を図４（ｄ）に示す。

【００５２】暗号化された応答パケットを受信した移動計算機２では、（暗号化パケットのヘッダにおける）送信元である境界ゲートウェイ４に対応する鍵で該パケットを復号し、得られた応答パケットから、登録に成功したことを認識する。

【００５３】以上のように、移動ＩＰの登録要求パケットが受諾されると、それ以降、移動計算機２のホームアドレス宛に送信されてきたパケットをホームネットワーク１１のパケット中継装置（移動計算機管理装置）５が捕捉し、これを移動計算機２の現在位置アドレス宛パケット内にカプセル化し、さらにこれを境界ゲートウェイ４に対応する鍵で暗号化して、境界ゲートウェイ４のプライベートアドレス宛に転送する。このパケット形式を図４（ｅ）に示す。なお、図４（ｅ）ではデータグラム（Ｄａｔａｇｒａｍ）の部分に通信相手発で移動計算機２のホームドレス宛のパケットがカプセル化される。そして、境界ゲートウェイ４は前述した位置登録の応答と同様にこのパケットを中継し、移動計算機宛に再暗号化して転送する。このパケット形式を図４（ｆ）に示す。

【００５４】また、移動計算機２が通信相手のサーバ７にパケットを送信する場合も、サーバ７のアドレスがホームネットワーク１１のパケット中継装置（移動計算機管理装置）５と同じポリシーで管理されるプライベートアドレスであるなら、前述の登録要求の場合と同様にして、移動計算機２は境界ゲートウェイ４対応の鍵で暗号化し、境界ゲートウェイ４のグローバルアドレス宛に送信する。そして、境界ゲートウェイ４は一度これを復号し、サーバ７宛のプライベートアドレスを用いた暗号化パケットに変換して転送する。

【００５５】このように、本実施形態に係る境界ゲートウェイ４により、グローバルネットワークとプライベートネットワークの境界で、２つの個別の暗号化転送路を構築することで、２つのアドレス空間を跨ぐ通信を可能とする。

【００５６】以上、本実施形態について説明してきたが、従来の移動ＩＰ方式では、移動計算機はホームネットワークとの到達可能性（ｒｅａｃｈａｂｉｌｉｔｙ）の保証された単一空間内でのみ移動が許されており、大規模な組織で組織内ネットワークをプライベートアドレスで構築している場合、組織外のグローバルアドレス領域に移動した計算機からは移動ＩＰ方式をそのまま使用できなかったが、本実施形態によれば、移動計算機側で自身の現在位置に応じて適切な形式でパケットを生成、送信するような制御を可能とし、また、組織ネットワークの入口で移動計算機からのパケットを一旦受信し、内容を確認して、組織内の該当するホームエージェント（パケット中継装置）宛に転送する処理を行うことにより、企業ネット等の組織ネットがプライベートアドレスで運用しており、移動計算機が組織外のグローバルアドレスに移動しても移動ＩＰ方式をそのまま使用し続ける

ことができる。

【００５７】一般に、大規模ネットワークでは、組織ネットの入口で通信内容のログを取ったりすることが多く、境界ゲートウェイの処理のオーバーヘッドは実際には問題にならない場合が多い。また、境界ゲートウェイでファイアウォールなどの他の制御機構を共存させる場合も拡張が容易である。

【００５８】また、本実施形態において、インターネットプロバイダなどに接続するシーケンス内で移動計算機のＩＰネットワーク上の位置を検出することで、移動計算機側の制御をさらに容易にできる。

【００５９】なお、本発明は、ＲＦＣ２００２に示される移動ＩＰだけでなく、他の様々な移動通信プロトコルに対しても適用可能である。また、以上の各機能は、ソフトウェアとしても実現可能である。また、本実施形態は、コンピュータに所定の手順を実行させるための（あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体として実施することもできる。本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【００６０】

【発明の効果】本発明によれば、移動計算機が本来属するホームネットワークとは異なるアドレス空間に移動した場合、移動計算機と境界ゲートウェイ等のパケット中継装置との間でそのアドレス空間におけるアドレスを用いて通信を行い、境界ゲートウェイ等のパケット中継装置とホームネットワーク内に位置するホームエージェント等の移動計算機管理装置やサーバ装置等のノードとの間でホームネットワークにおけるアドレスを用いて通信を行うので、移動計算機が組織外のグローバルアドレスに移動しても移動ＩＰ方式をそのまま使用し続けることができる。

【図面の簡単な説明】

【図１】本実施形態に係るネットワークの基本構成を示す図

【図２】制御パネルの一例を示す図

【図３】制御パネルの他の例を示す図

【図４】パケット形式の例を示す図

【図５】管理テーブルの一例を示す図

【図６】移動ＩＰ方式について説明するための図

【符号の説明】

１…組織ネットワーク

２…移動計算機

５…パケット中継装置（移動計算機管理装置）

６…インターネット

４…境界ゲートウェイ

７…サーバ

１１…ホームネットワーク

フロントページの続き

(72)発明者　津田　悦幸
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内